MATH 314 Spring 2020 - Class Notes

01/29/2020

Scribe: Andrew Noonan

Summary: The Affine Cipher and cryptoanalysis. The Affine Cipher is a mono-alphabetic cipher with the key (α, β)

Notes:

- Affine Cipher Encryption / Decryption
  - Keys (α, β), where α != even or 13 and $0 \leq \beta \leq 25$(312 possibilities)
  - E(X) = $\alpha x + \beta$
  - D(y) = $(\alpha^{-1} y) - \beta$
- Attacking Affine
  1. Chosen Plaintext

     Pick α to be a (0) and read off β

     E(0) = $\alpha(0) + \beta \equiv \beta$

     Pick α to be b (1) then subtract β from the Ciphertext E(b)

     E(1) = α (1) $+\beta$

     α = E(1) $-\beta$
  2. Known plaintext

     See examples
  3. Ciphertext only

     Brute force can be used to break the cipher since there are only 312 possibilities for K (12 α's, 25 β's)
- Theorems
  1. $A|B$

     Definiton: 'A divides B' if $b = ka$, where k $\in \mathbb{Z}$
  2. A $\equiv$ B (mod M)

     Defintion: 'A is equivalent to B (mod M)' if $n|(a - b)$
  3. It is possible to add, subtract, and multiply, however, you cannot divide in mod M (This requires an inverse)

Examples: Encryption — Decryption — Known Plaintext Attack

- cup encrypts to OYB

  $E(2) \equiv \alpha(2) + \beta \equiv 14$

  $E(20) \equiv \alpha(20) + \beta \equiv 23$

  $E(15) \equiv \alpha(15) + \beta \equiv 1$

- find inverse of α, then find α:

  $\alpha(20) + \beta \equiv 24$

  - $\alpha(15) + \beta \equiv 1$

  $5^{-1} \equiv 21$

  $\alpha(5) * 5^{-1} \equiv 23 * 21 \equiv 15(mod 26)$

  $\alpha \equiv 15$

- find β

  $E(2) \equiv 15(2) + \beta \equiv 14(mod 26)$

  $E(2) \equiv 4 + \beta \equiv 14(mod 26)$

  $E(2) \equiv \beta \equiv 10(mod 26)$

- $E(x) \equiv 15(x) + 10(mod 26)$